



DEPARTMENT OF THE ARMY
INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, UNITED STATES ARMY GARRISON-DETROIT ARSENAL
6501 E. ELEVEN MILE ROAD
WARREN MI 48397-5000

30 MAR 2009

IMNE-MIG-IMA

MEMORANDUM FOR U.S. Army Garrison-Detroit Arsenal and All Tenants and Liaison Activities

SUBJECT: Policy Memorandum #22, Network Information Assurance Vulnerability Management Program Policy

1. REFERENCES.

- a. AR-25-2, Information Assurance, 24 Oct 2007.
- b. DODI 8500.2, Information assurance (IA) Implementation, 6 Feb 2003.
- c. Memorandum AMSTA-CS-X U.S. Army Garrison-Michigan (USAG-M) Computer Security dated 22 Nov 04 (Superseded by this memorandum)
- d. Department of the Army Vice Chief of Staff Memorandum, Subject: Army Energy Conservation dated 22 June 2007.

2. PURPOSE. The purpose of this memorandum is to provide guidance to all U.S. Army Garrison-Detroit Arsenal (USAG-DTA) personnel on Network Information Assurance Vulnerability Management.

3. APPLICABILITY. Compliance with the Information Assurance Vulnerability Management (IAVM) program outlined in references (a) and (b) is required for all Information Systems (IS) and devices that connect to Army networks.

4. POLICY. The Directorate of Information Management (DOIM) maintains a process for continually updating network systems and ensuring compliance. Non-compliant computers must be updated or they will be disconnected from the network.

5. PROCEDURES.

a. Effective immediately the installation of software patches and updates will be executed automatically when the user logs on to the computer. If the user does not logon, then the installation will occur at 1200 noon daily as long as the computer is powered on. The 0300 (a.m.) policy outlined in reference (c) is hereby rescinded.

b. Current efforts to maintain Information Assurance Vulnerability Alert (IAVA) and Antivirus (AV) compliance are not meeting Army goals. Users must make all efforts to ensure

IMNE-MIG-IMA

SUBJECT: Policy Memorandum #22, Network Information Assurance Vulnerability Management Program Policy

their computers are made available to receive automated patches and updates. Computers must be powered-on for patch installation to occur. Users are asked to not turn the computer off until after the installation is complete. The user may be prompted to reboot the computer after the patch is installed or given an option to do so later. A reminder will reappear until this action is complete or the computer is powered off by the user.

c. Computers that have not connected to the network for more than 30 calendar days will be deleted from the network active directory unless prior coordination is made with the DOIM. To re-join the network, service tickets must be submitted to the DOIM Helpdesk.

d. Computers that are deployed or on extended TDY beyond 30 days must be identified prior to departure to the DOIM Helpdesk by the user's parent organization. The user is responsible for ensuring that the computer is compliant with updated patches before departure.

e. System owners of mission applications are required to participate in the Army IAVM program by subscribing to the Army IAVM Forum (formerly known as the Army IAVM COMMUNITY) located on AKO. System owners should review all IAVAs and coordinate actions with the DOIM to avoid adverse impact on their applications.

6. PROPONENT. DOIM Information Assurance Division is the proponent office for this USAG-DTA policy. Point of contact (POC) is the installation Senior Information Assurance Manager at DSN 786-5561 or commercial (586) 574-5561.


BRENDA LEE MCCULLOUGH
Garrison Manager